Appropriate Monitoring for Schools

June 2017

Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" . Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	Schools Broadband in partnership with Netsweeper
Address	Units 2 – 4 Backstone Business Park, Dansk Way, Ilkley, LS29 8JZ
Contact details	01133 222 333
Filtering System	Netsweeper
Date of assessment	August 2017

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		The filter categorises sites of this nature, including language and imagery. It enables schools to allow or block the website depending on the school's policy.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		The filter categorises language and imagery relating to this subject.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		The filter categorises language and imagery relating to this subject.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		The filter categorises sites of this nature. It categorises language and imagery relating to this subject. Schools may allow or block depending on the school's policy.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		The filter categorises sites of this nature. It categorises language and imagery relating to this subject. Schools may allow or block depending on the school's policy.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The filter categorises sites of this nature. It categorises language and imagery relating to this subject. Schools may allow or block depending on the school's policy.
Pornography	displays sexual acts or explicit images		The filter categorises sites of this nature. It categorises language and imagery relating to this subject. Schools may allow or block depending on the school's policy.
Self Harm	promotes or displays deliberate self harm		The filter categorises sites of this nature. It categorises language and imagery relating to this subject.

			Schools may allow or block depending on the school's policy
Suicide	Suggest the user is considering suicide		The filter categorises sites of this nature. It categorises language and
Violence	Displays or promotes the use of physical force intended to hurt or kill		The filter categorises sites of this nature. It categorises language and imagery relating to this subject. Schools may allow or block depending on the school's policy

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

All websites are categorised and schools have the ability to manage which categories they choose to block or allow. Schools can also allow or block individual websites by using URL overrides. Anything not categorised will appear in the unknown list where schools can choose to allow or block.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Giving schools direct access to the filters means they can tailor their own browsing experience. We will always provide assistance where required.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to		Schools have ability to set users at different web filter levels generally dictated by age
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		The system has full support for BYOD networks should the school choose to deploy them. Same levels of filtering apply to non BYOD devices.
• Data retention –what data is stored, where and for how long		All data is stored for in our secure data centre should a school need to access it. Information includes client IPs, User Names, Browsing Activity & Date Time Stamps plus more
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Yes, customers are advised which devices and operating systems are covered by the filtering platform

• Flexibility – schools ability to amend (add or remove) keywords easily		Schools have direct control of their filtering which is assisted by our support Dept. if necessary.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Block messages are displayed on all block request pages. Full support for any replacement messages is included & we will provide advice where required.
• Multiple language support – the ability for the system to manage relevant languages?		Yes
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		The school can set a dedicated email address for any alerts to go to should certain events be triggered.
• Reporting – how alerts are recorded within the system?		Emailed to dedicated address and stored within report data.

Please note below opportunities to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

Schools Broadband has a strategic partnership with one of the country's most renowned online safety experts. This partnership gives us access to immediate and up to date advice on all issues relating to "Keeping Children Safe in Education." Our termly newsletter has a regular feature on statutory guidance updates. We also run invaluable and informative online safety seminars for schools offering guidance on how to develop school policies.

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Ben Smith
Position	Sales Director
Date	14/08/2017
Signature	